On the Direct Sum Conjecture

Ephraim Feig and Shmuel Winograd
Mathematical Sciences Department
IBM Thomas J. Watson Research Center
Yorktown Heights, New York 10598

Submitted by Hans Schneider

ABSTRACT

We prove the direct sum conjecture for various sets of systems of bilinear forms. Our results depend on *a priori* knowledge of the complexity of at least one of the direct summands and its underlying algebraic structure. We also briefly survey some previous results concerning the complexity and structure of minimal algorithms for various direct sum systems.

I. INTRODUCTION

Let G be a field, and let $x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s$ be indeterminants over G. A system $\mathscr{B} = \{B_1, B_2, \ldots, B_t\}$ of bilinear forms is given by

$$B_k = \sum_{j=1}^{s} \sum_{i=1}^{r} g_{ijk} x_i y_j, \qquad k = 1, 2, \ldots, t,$$

where the g_{ijk}'s are elements of G. The system $\mathscr{B}$ can be written as

$$\mathscr{B} = A(\mathbf{x})\mathbf{y},$$

where $A(\mathbf{x})$ is the $t \times s$ matrix whose (k, j) entry is $L_{kj}(\mathbf{x}) = \sum_{i=1}^{r} g_{ijk} x_i$, and where $\mathbf{y}$ is the (column) vector $\mathbf{y} = (y_1, \ldots, y_s)^T$. Alternatively, we can write $\mathscr{B}$ as

$$\mathscr{B} = \mathbf{x}^T \bar{A}(\mathbf{y}),$$

where $\bar{A}(\mathbf{y})$ is the $r \times t$ matrix whose (i, k) entry is $\bar{L}_{ik}(\mathbf{y}) = \sum_{j=1}^{s} g_{ijk} y_j$, and $\mathbf{x}^T = (x_1, x_2, \ldots, x_r)$.

52 Vanderbilt Ave., New York, NY 10017 0024-3795/84/$3.00

If $\mathscr{B}$ is defined by multiplication in an associative algebra, then $A(\mathbf{x})$ and $\bar{A}(\mathbf{y})$ are the operators of left and right multiplication by $\mathbf{x}$ and $\mathbf{y}$ respectively.

Let $x_1,\ldots,x_r; y_1,\ldots,y_s$ and $\xi_1,\ldots,\xi_{r'}; \eta_1,\ldots,\eta_{s'}$ be distinct indeterminants. Let $\mathscr{B} = A(\mathbf{x})\mathbf{y}$ and $\mathscr{B}' = A'(\boldsymbol{\xi})\boldsymbol{\eta}$ be two systems of bilinear forms. Define $\tilde{\mathscr{B}} = \mathscr{B} \oplus \mathscr{B}'$, the *direct sum of* $\mathscr{B}$ *and* $\mathscr{B}'$, by

$$A(\mathbf{x})\mathbf{y} \oplus A'(\boldsymbol{\xi})\boldsymbol{\eta} = \begin{pmatrix} A(\mathbf{x}) & 0 \\ 0 & A'(\boldsymbol{\xi}) \end{pmatrix} \begin{pmatrix} \mathbf{y} \\ \boldsymbol{\eta} \end{pmatrix}.$$

The reader should note that although $A(\cdot)$ and $A'(\cdot)$ may be the same matrix, all the indeterminants must be distinct.

A (*bilinear*) *algorithm* $\mathscr{A}$ is a set $\{m_1(\mathbf{x},\mathbf{y}),\ldots,m_n(\mathbf{x},\mathbf{y})\}$, where

$$m_l(\mathbf{x},\mathbf{y}) = L_l(\mathbf{x})L_l'(\mathbf{y}) = \left(\sum_{i=1}^{r} a_{i,l}x_i\right)\left(\sum_{j=1}^{s} b_{j,l}y_j\right), \qquad l = 1,2,\ldots,n.$$

($a_{i,l} \in G$, $b_{j,l} \in G$ for $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$, $1 \leqslant l \leqslant n$.) The algorithm $\mathscr{A}$ *can compute* $\mathscr{B} = \{B_1,\ldots,B_t\}$ if $\{B_1,\ldots,B_t\}$ is a subset of $L_G(m_1(\mathbf{x},\mathbf{y}),\ldots,m_n(\mathbf{x},\mathbf{y}))$—the G-linear span of $\{m_1(\mathbf{x},\mathbf{y}),\ldots,m_n(\mathbf{x},\mathbf{y})\}$. In other words, there exists a $t \times n$ G-matrix C such that

$$\mathscr{B} = A(\mathbf{x})\mathbf{y} = C\mathbf{m},$$

where $\mathbf{m}$ is the (column) vector $\mathbf{m} = (m_1(\mathbf{x},\mathbf{y}),\ldots,m_n(\mathbf{x},\mathbf{y}))^T$.

We denote n by $\bar{\mu}(\mathscr{A})$ and define

$$\bar{\mu}(A(\mathbf{x})\mathbf{y}) = \min(\bar{\mu}(\mathscr{A})),$$

where the minimization is over all algorithms which compute $A(\mathbf{x})\mathbf{y}$. An algorithm $\mathscr{A}$ which computes $\mathscr{B}$ is called *minimal* if $\bar{\mu}(\mathscr{A}) = \bar{\mu}(\mathscr{B})$.

Strassen [1], and Fiduccia and Zalkstein [2], conjectured that

$$\bar{\mu}(A(\mathbf{x})\mathbf{y} \oplus A'(\boldsymbol{\xi})\boldsymbol{\eta}) = \bar{\mu}(A(\mathbf{x})\mathbf{y}) + \bar{\mu}(A'(\boldsymbol{\xi})\boldsymbol{\eta}).$$

Let $\mathscr{A} = \{m_1(\mathbf{x},\mathbf{y}),\ldots,m_n(\mathbf{x},\mathbf{y})\}$ be an algorithm for computing $A(\mathbf{x})\mathbf{y}$, i.e. $A(\mathbf{x})\mathbf{y} = C\mathbf{m}$; and let $\mathscr{A}' = \{m_1'(\boldsymbol{\xi},\boldsymbol{\eta}),\ldots,m_{n'}'(\boldsymbol{\xi},\boldsymbol{\eta})\}$ be an algorithm for computing $A'(\boldsymbol{\xi})\boldsymbol{\eta}$, i.e. $A'(\boldsymbol{\xi})\boldsymbol{\eta} = C'\mathbf{m}'$. The algorithm $\tilde{\mathscr{A}} = \mathscr{A} \oplus \mathscr{A}' = \{m_1(\mathbf{x},\mathbf{y}),\ldots,m_n(\mathbf{x},\mathbf{y}), m_1'(\boldsymbol{\xi},\boldsymbol{\eta}),\ldots,m_{n'}'(\boldsymbol{\xi},\boldsymbol{\eta})\}$, called the *direct sum of* $\mathscr{A}$ *and* $\mathscr{A}'$, computes $A(\mathbf{x})\mathbf{y} \oplus A'(\boldsymbol{\xi})\boldsymbol{\eta}$. It is therefore immediate that for every $\mathscr{B}$ and

$\mathscr{B}'$ we have

$$\bar{\mu}(\mathscr{B}\oplus\mathscr{B}') \leqslant \bar{\mu}(\mathscr{B})+\bar{\mu}(\mathscr{B}').$$

If equality holds, we say that $\mathscr{B}$ and $\mathscr{B}'$ *satisfy the direct sum conjecture.*

Let $\mathscr{B}$ and $\mathscr{B}'$ satisfy the direct sum conjecture. The algorithm $\tilde{\mathscr{A}} = \mathscr{A}\oplus\mathscr{A}'$ is a minimal algorithm for $\mathscr{B}\oplus\mathscr{B}'$ whenever $\mathscr{A}$ is a minimal algorithm for $\mathscr{B}$, and $\mathscr{A}'$ is a minimal algorithm for $\mathscr{B}'$. If every minimal algorithm for $\mathscr{B}\oplus\mathscr{B}'$ is a direct sum algorithm, we say that $\mathscr{B}$ and $\mathscr{B}'$ *satisfy the direct sum conjecture strongly.*

Hopcroft and Kerr [3] studied the complexity of the product of 2×2 by $2\times n$ matrices. Let us denote by $\langle m,n,p\rangle$ the system of bilinear forms $\{B_{ik} | 1\leqslant i\leqslant m,\ 1\leqslant k\leqslant p\}$, where $B_{ik}=\sum_{j=1}^{n} x_{ij}y_{jk}$ for all $1\leqslant i\leqslant m$ and $1\leqslant k\leqslant p$. Hopcroft and Kerr showed that if $G=\mathrm{GF}(2)$ then $\bar{\mu}(\langle 2,2,2n\rangle)=7n$. Because every algorithm for computing the n-fold direct sum $\langle 2,2,2\rangle\oplus\langle 2,2,2\rangle\oplus\cdots\oplus\langle 2,2,2\rangle = n\langle 2,2,2\rangle$ yields an algorithm for computing $\langle 2,2,2n\rangle$, we have

$$\begin{aligned} 7n=\bar{\mu}(\langle 2,2,2n\rangle) &\leqslant \bar{\mu}(n\langle 2,2,2\rangle) \\ &\leqslant n\bar{\mu}(\langle 2,2,2\rangle)=7n. \end{aligned}$$

That is, when $G=\mathrm{GF}(2)$, n copies of $\langle 2,2,2\rangle$ satisfy the direct sum conjecture.

Let $P(u)\in G[u]$ be a polynomial of degree n. We denote by $\mathscr{B}(P)=\{B_0, B_1,\ldots, B_{n-1}\}$ the system of bilinear forms defined by

$$\sum_{i=0}^{n-1} B_i u^i = \left(\sum_{i=0}^{n-1} x_i u^i\right)\left(\sum_{i=0}^{n-1} y_i u^i\right) \bmod P(u);$$

that is, $\mathscr{B}(P)$ is the system of coefficient of the product of two polynomials modulo $P(u)$. Winograd [4] investigated the complexity of $\mathscr{B}(P)$ when $P(u)=Q(u)^l$ and $Q(u)$ is irreducible over G. It was shown in [4] that if $P_i(u)=Q_i(u)^{l_i}$, $i=1,2,\ldots,k$, where the Q_i's are (not necessarily distinct) irreducible polynomials, then

$$\bar{\mu}(\mathscr{B}(P_1)\oplus\cdots\oplus\mathscr{B}(P_k)) = \bar{\mu}(\mathscr{B}(P_1))+\cdots+\bar{\mu}(\mathscr{B}(P_k)) = 2\sum_{i=1}^{k} n_i - k,$$

where $n_i=\deg(P_i)$, provided that the cardinality of G satisfies $|G|\geqslant$

$2\max_i\{n_i\}-1$. That is, under the assumption on $|G|$, $\mathscr{B}(P_1),\ldots,\mathscr{B}(P_k)$ satisfy the direct sum conjecture. It was also shown in [4] that under the same assumption $\mathscr{B}(P_1),\ldots,\mathscr{B}(P_k)$ satisfy the direct sum conjecture strongly. (The results of [4] are stronger than stated here, for they deal with quadratic algorithms not just bilinear ones. But as this paper deals only with bilinear algorithms, we did not state the results in their full generality.)

The results of [4] were extended by Auslander, Feig, and Winograd [5]. For any polynomial $P(u)\in G[u]$ of degree n, and positive integer r, we define the system $\mathscr{B}(P,r)=\{B_i^{(j)}|\ 0\leqslant i\leqslant n-1,\ 1\leqslant j\leqslant r\}$ by

$$\sum_{i=0}^{n-1} B_i^{(j)}u^i=\left(\sum_{i=0}^{n-1} x_iu^i\right)\left(\sum_{i=0}^{n-1} y_i^{(j)}u^i\right) \bmod P(u), \qquad 1\leqslant j\leqslant r.$$

(Note that while the y-indeterminants are indexed by i and j, the x-indeterminants are indexed by i only.) The results of [5], together with those of [6], show that if $P_1(u),\ldots,P_k(u)$ are (not necessarily distinct) irreducible polynomials over G, then

$$\begin{aligned}\bar{\mu}\big(\mathscr{B}(P_1,r_1)\oplus\cdots\oplus\mathscr{B}(P_k,r_k)\big)&=\sum_{j=1}^{k}\bar{\mu}\big(\mathscr{B}(P_j,r_j)\big)\\&=\sum_{j=1}^{k} r_j\big[2\deg(P_j)-1\big],\end{aligned}$$

provided that $|G|\geqslant 2\max_j\{\deg(P_j)\}-2$. Moreover, under the same assumption on $|G|$, $\mathscr{B}(P_1,r_1),\mathscr{B}(P_2,r_2),\ldots,\mathscr{B}(P_k,r_k)$ satisfy the direct sum conjecture strongly.

In the next section we will describe preliminary results and constructions which will be needed in the rest of the paper. In Section III we will use these tools to prove two direct sum theorems. One consequence of these theorems is that for any system of bilinear forms $\mathscr{B}$, $\mathscr{B}$ and $\mathscr{B}_Q$ satisfy the direct sum conjecture. Here $\mathscr{B}_Q=\{B_0,B_1,B_2,B_3\}$ is the system of bilinear forms under multiplication of quaternions, i.e.,

$$B_0+iB_1+jB_2+kB_3=(x_0+ix_1+jx_2+kx_3)(y_0+iy_1+jy_2+ky_3)$$

where $i^2=j^2=k^2=-1$ and $ij=-ji=k$.

In Section III we will generalize the result of [4]. The main result of this section is that for any system of bilinear forms $\mathscr{B}$, and for any irreducible polynomial $Q(u)\in G[u]$, $\mathscr{B}$ and $\mathscr{B}(Q^l)$ satisfy the direct sum conjecture strongly, provided $|G|\geqslant 2l\deg(Q)-2$.

The main result of Section IV is that $\mathscr{B}$ and $\langle 2,2,2\rangle$ satisfy the direct sum conjecture strongly, provided that $|G| \geqslant 3$. Here, again, $\mathscr{B}$ is an arbitrary system of bilinear forms.

II. PRELIMINARY RESULTS

We will begin this section with some notation and definitions.

Let $Z = \{z_1, z_2, \ldots, z_n\}$ be a set. We will use $\mathscr{L}_G(Z)$ to denote the G-linear space generated by Z, and $\dim \mathscr{L}_G(Z)$ to denote its dimension.

Let $x_1, x_2, \ldots, x_n$ be indeterminants (over G), and let $L(\mathbf{x}) = \sum_{i=1}^{n} g_i x_i$ be a linear form. Let $I \subseteq \{1,2,\ldots,n\}$ be an index set. We use $L'(\mathbf{x}) = L(\mathbf{x})|x_i = \alpha_i$, $i \in I$, to denote the linear form obtained by substituting α_i for x_i $(i \in I)$; that is, $L'(\mathbf{x}) = \sum_{i \notin I} g_i x_i + \sum_{i \in I} g_i \alpha_i$.

DEFINITION 2.1. Let $\{L_1(\mathbf{x}), \ldots, L_n(\mathbf{x})\}$ be a set of linear forms. We say that it *depends on* x_i, $i \in I$, if $\dim \mathscr{L}_G(\{L_j(\mathbf{x})|x_i = 0,\ i \notin I\}) = |I|$, where $|I|$ denotes the cardinality of I.

The reader should note that $\{L_1(\mathbf{x}), \ldots, L_n(\mathbf{x})\}$ may depend on $\{x_1\}$ and on $\{x_2\}$ but not on $\{x_1, x_2\}$.

DEFINITION 2.2. Let $\mathscr{B} = A(\mathbf{x})\mathbf{y} = \mathbf{x}^T\hat{A}(\mathbf{y})$ be a system of bilinear forms. We say that $\mathscr{B}$ *depends on* $\{x_i|i \in I\}$ $[\{y_j|j \in J\}]$ if the entries of $A(\mathbf{x})$ $[\hat{A}(\mathbf{y})]$ depend on $\{x_i|i \in I\}$ $[\{y_j|j \in J\}]$.

REMARK. Let $c_1(\mathbf{x}), \ldots, c_k(\mathbf{x})$ be the first k columns of $A(\mathbf{x})$. $\mathscr{B}$ depends on $\{y_1, \ldots, y_k\}$ if and only if $k = \dim \mathscr{L}_G(\{c_1(\mathbf{x}), \ldots, c_k(\mathbf{x})\})$.

DEFINITION 2.3. Let $\mathscr{A} = (m_1(\mathbf{x},\mathbf{y}), \ldots, m_n(\mathbf{x},\mathbf{y}))$ be an algorithm, where $m_i(\mathbf{x},\mathbf{y}) = L_i(\mathbf{x})L_i'(\mathbf{y})$, $1 \leqslant i \leqslant n$. We say that $\mathscr{A}$ *depends on* $\{x_i|i \in I\}$ $[\{y_j|j \in J\}]$ if $\{L_1(\mathbf{x}), \ldots, L_n(\mathbf{x})\}$ $[\{L_1'(\mathbf{y}), \ldots, L_n'(\mathbf{y})\}]$ depend on $\{x_i|i \in I\}$ $[\{y_j|j \in J\}]$.

Let $\mathscr{B}$ be a system of bilinear forms, and let $\mathscr{A}$ be an algorithm which computes $\mathscr{B}$. If $\mathscr{B}$ depends on $\{x_i|i \in I\}$ $(\{y_j|j \in J\})$ then so does $\mathscr{A}$. In particular, that means that $n = \bar{\mu}(\mathscr{A})$ satisfies $n \geqslant |I|$ and $n \geqslant |J|$. This is a special case of the column rank theorem. So we now state:

THEOREM (Column rank). *Let* $A(\mathbf{x})\mathbf{y}$ *be a system of bilinear forms. Let* $c_1(\mathbf{x}), \ldots, c_s(\mathbf{x})$ *denote the columns of* $A(\mathbf{x})$. *Then*

$$\bar{\mu}(A(\mathbf{x})\mathbf{y}) \geqslant \dim \mathscr{L}_G(\{c_1(\mathbf{x}), \ldots, c_s(\mathbf{x})\}).$$

It can happen that $\mathscr{A}$ depends on $\{x_i | i \in I\}$ ($\{y_j | j \in J\}$) while the system of bilinear forms which $\mathscr{A}$ computes does not. Lemma 8 of [5] shows an important case when this cannot happen. We cite this lemma without proof.

LEMMA 2.1. *Let $\mathscr{A}$ be a minimal algorithm for computing $\mathscr{B}$. If $\mathscr{A}$ depends on $\{x_i | i \in I\}$ ($\{y_j | j \in J\}$) then so does $\mathscr{B}$.*

DEFINITION 2.4. Let $\mathscr{A} = (m_1, m_2, \ldots, m_n)$ be an algorithm, where $m_i = m_i(\mathbf{x}, \boldsymbol{\xi}; \mathbf{y}, \boldsymbol{\eta}) = L_i(\mathbf{x}, \boldsymbol{\xi}) L_i'(\mathbf{y}, \boldsymbol{\eta})$, $1 \leqslant i \leqslant n$. We say that $\mathscr{A}$ *mixes* $\mathbf{x}$ and $\boldsymbol{\xi}$ [$\mathbf{y}$ and $\boldsymbol{\eta}$] if for some $i = 1, 2, \ldots, n$, $L_i(\mathbf{x}, \boldsymbol{\xi})$ [$L_i'(\mathbf{y}, \boldsymbol{\eta})$] depends on some $\{x_j\}$ and $\{\xi_k\}$ [$\{y_j\}$ and $\{\eta_k\}$]. If $\mathscr{A}$ does not mix $\mathbf{x}$ and $\boldsymbol{\xi}$ [$\mathbf{y}$ and $\boldsymbol{\eta}$], we say that $\mathscr{A}$ is *partitioned* by $\mathbf{x}$ and $\boldsymbol{\xi}$ [$\mathbf{y}$ and $\boldsymbol{\eta}$].

We will now cite another lemma of [5], lemma 9, without proof.

LEMMA 2.2. *Let $\mathscr{A}$ be an algorithm for computing $A(\mathbf{x})\mathbf{y} \oplus A'(\boldsymbol{\xi})\boldsymbol{\eta}$. If*

(1) $\bar{\mu}(\mathscr{A}) \leqslant \bar{\mu}(A(\mathbf{x})\mathbf{y}) + \bar{\mu}(A'(\boldsymbol{\xi})\boldsymbol{\eta})$ *and*
(2) $\mathscr{A}$ *is partitioned by* $\mathbf{x}$ *and* $\boldsymbol{\xi}$ ($\mathbf{y}$ *and* $\boldsymbol{\eta}$),

then $\mathscr{A}$ is a direct sum algorithm, $\mathscr{A} = \mathscr{A}' \oplus \mathscr{A}''$, where $\mathscr{A}'$ computes $A(\mathbf{x})\mathbf{y}$ and $\mathscr{A}''$ computes $A'(\boldsymbol{\xi}')\boldsymbol{\eta}'$; therefore

$$\bar{\mu}(\mathscr{A}) = \bar{\mu}(A(\mathbf{x})\mathbf{y}) + \bar{\mu}(A'(\boldsymbol{\xi})\boldsymbol{\eta}).$$

The main technique which we will use to prove the results is that of substitution. We will now describe the two kinds of substitution which we will employ.

Indeterminant Substitution

Let $A(\mathbf{x})\mathbf{y}$ be a system of bilinear forms, where $\mathbf{x} = (x_1, \ldots, x_r)^T$ and $\mathbf{y} = (y_1, \ldots, y_s)^T$. Let $\mathscr{A} = (m_1(\mathbf{x}, \mathbf{y}), \ldots, m_n(\mathbf{x}, \mathbf{y}))$ be an algorithm for computing $A(\mathbf{x})\mathbf{y}$, $m_i(\mathbf{x}, \mathbf{y}) = L_i(\mathbf{x}) L_i'(\mathbf{y})$, $1 \leqslant i \leqslant n$. Assume that $A(\mathbf{x})\mathbf{y}$ depends on $\{x_i | i \in I\}$ [$\{y_j | j \in J\}$]. To avoid cumbersome notation we assume the set on which $A(\mathbf{x})\mathbf{y}$ depends to be $\{x_1, \ldots, x_k\}$ [$\{y_1, \ldots, y_k\}$]. Because $\mathscr{A}$ computes $A(\mathbf{x})\mathbf{y}$, it too depends on $\{x_1, \ldots, x_k\}$ [$\{y_1, \ldots, y_k\}$]. That means that there are k $L_i'(\mathbf{y})$'s [$L_i'(\mathbf{y})$'s], say $L_1(\mathbf{x}), \ldots, L_k(\mathbf{x})$ [$L_1'(\mathbf{y}), \ldots, L_k'(\mathbf{y})$], such that $\{L_1(\mathbf{x}), \ldots, L_k(\mathbf{x})\}$ [$\{L_1'(\mathbf{y}), \ldots, L_k'(\mathbf{y})\}$] also depends on $\{x_1, \ldots, x_k\}$ [$\{y_1, \ldots, y_k\}$].

We will now drop the tiresome attempt to describe the process in terms of both the x-indeterminants and the y-indeterminants. We will consider only the x's and trust the reader to fill in the y's.

Let $L_i(\mathbf{x}) = \sum_{j=1}^{r} a_{ij}x_j$, $1 \leqslant i \leqslant k$. Then the vector $L = (L_1(\mathbf{x}), \ldots, L_k(\mathbf{x}))^T$ can be written as $L = M\mathbf{x}(k) + N\hat{\mathbf{x}}(k)$. Here M is the $k \times k$ G-matrix $M_{ij} = a_{ij}$, $1 \leqslant i, j \leqslant k$; N is the $k \times (r-k)$ G-matrix $N_{ij} = a_{i,k+j}$, $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant r-k$; $\mathbf{x}(k)$ is the (column) vector $\mathbf{x}(k) = (x_1, \ldots, x_k)^T$; and $\hat{\mathbf{x}}(k)$ is the (column) vector $\hat{\mathbf{x}}(k) = (x_{k+1}, \ldots, x_r)^T$. Because $\mathscr{L}_G\{L_1(\mathbf{x}), \ldots, L_k(\mathbf{x})\} = \mathscr{L}_G\{x_1, \ldots, x_k\}$, we have that M is a nonsingular matrix. We define $\mathbf{x}'(k) = (x_1', x_2', \ldots, x_k')^T$ by

$$\mathbf{x}_1'(k) = -M^{-1}N\hat{\mathbf{x}}(k).$$

It should be emphasized that $x_1', \ldots, x_k'$ are not indeterminants, but linear forms of the indeterminants $x_{k+1}, \ldots, x_r$.

We now define a new system of bilinear forms $\mathscr{B}'$. The system $\mathscr{B}'$ is obtained from $\mathscr{B}$ by setting $x_i = x_i'$, $1 \leqslant i \leqslant k$. As it will be important to analyze $\bar{\mu}(\mathscr{B}')$, we will now describe it in more detail. In the case (described above) that we substituted for x-indeterminants, let $A'(\mathbf{x})$ be the $t \times s$ matrix $A'(\mathbf{x}) = A(\mathbf{x})|_{x_i = x_i',\, 1 \leqslant i \leqslant k}$. The system $\mathscr{B}'$ is $\mathscr{B}' = A'(\mathbf{x})\mathbf{y}$. In the case (which the reader filled in) where we substituted for y-indeterminants, we use $A_k(\mathbf{x})$ to denote the $t \times k$ matrix whose columns are the first k columns of $A(\mathbf{x})$. We now set $A'(\mathbf{x}) = \hat{A}_k(\mathbf{x}) - A_k(\mathbf{x})M^{-1}N$. The system $\mathscr{B}'$ is $\mathscr{B}' = A'(\mathbf{x})\hat{\mathbf{y}}(k)$, where $\hat{\mathbf{y}}(k) = (y_{k+1}, \ldots, y_s)^T$.

In either case, we also have an algorithm $\mathscr{A}'$ which can compute $\mathscr{B}'$; namely, the algorithm obtained by substituting x_i' for x_i (y_i' for y_i), $1 \leqslant i \leqslant k$, in each $m_j(\mathbf{x}, \mathbf{y})$ of $\mathscr{A}$, $1 \leqslant j \leqslant n$. By construction, this substitution annihilates $m_1(\mathbf{x}, \mathbf{y}), \ldots, m_k(\mathbf{x}, \mathbf{y})$, so $\bar{\mu}(\mathscr{A}') \leqslant n - k$. We thus obtain that

$$\bar{\mu}(\mathscr{B}') \leqslant \bar{\mu}(\mathscr{A}) - k.$$

It is important to notice that $\mathscr{B}'$ is specified not only by $A(\mathbf{x})\mathbf{y}$ and $\{x_i | i \in I\}$ [or $\{y_j | j \in J\}$], but also by the algorithm $\mathscr{A}$, and by the choice of $L_1(\mathbf{x}), \ldots, L_k(\mathbf{x})$ [or $L_1'(\mathbf{y}), \ldots, L_k'(\mathbf{y})$].

We denote by $\mathscr{B}'$ the system obtained from $\mathscr{B}$ by removing $x_1, \ldots, x_k$ [$y_1, \ldots, y_k$] using $L_1(\mathbf{x}), \ldots, L_k(\mathbf{x})$ [$L_1'(\mathbf{y}), \ldots, L_k'(\mathbf{y})$].

We will end the description of the substitution of indeterminants by observing that if $\{L_1(\mathbf{x}), \ldots, L_k(\mathbf{x})\}$ depends on $\{x_i | i \in I \subseteq \{k+1, \ldots, r\}\}$, then so does $\{x_1', \ldots, x_k'\}$.

Substitution of Bilinear Forms

Let $\mathscr{B} = \{B_1, \ldots, B_t\} = A(\mathbf{x})\mathbf{y}$ be a system of bilinear forms, and let $\mathscr{A} = (m_1(\mathbf{x},\mathbf{y}), \ldots, m_n(\mathbf{x},\mathbf{y}))$ be an algorithm which computes it. That is, $A(\mathbf{x})\mathbf{y} = C\mathbf{m}$ for some $t \times n$ G-matrix C, where $\mathbf{m}$ is the (column) vector $\mathbf{m} = (m_1(\mathbf{x},\mathbf{y}), \ldots, m_n(\mathbf{x},\mathbf{y}))^T$.

We now assume that $B_1, B_2, \ldots, B_k$ are G-linearly independent; that is, we assume that $k = \dim \mathscr{L}_G(\{B_1, \ldots, B_k\})$. This assumption is the same as assuming that the first k rows of $A(\mathbf{x})$ are G-linearly independent. Let $A_1(\mathbf{x})$ be the $k \times s$ matrix whose rows are the first k rows of $A(\mathbf{x})$, and let $A_2(\mathbf{x})$ be the $(t-k)\times s$ matrix whose rows are the last $t-k$ rows of $A(\mathbf{x})$. With this notation we have

$$A_1(\mathbf{x})\mathbf{y} = C_1\mathbf{m} \quad \text{and} \quad A_2(\mathbf{x})\mathbf{y} = C_2\mathbf{m},$$

where the $k \times n$ matrix C_1 and the $(t-k)\times n$ matrix C_2 are obtained from C in the obvious way. The assumption that the rows of $A_1(\mathbf{x})$ are G-linearly independent implies that $k = \operatorname{rank}(C_1)$. Therefore, there are k columns of C_1 which are linearly independent, and without loss of generality we assume that they are the first k columns. So we can write C_1 as $C_1 = (C_1'|C_1'')$ where C_1' is a $k \times k$ nonsingular matrix.

Using this notation we can now write

$$A_1(\mathbf{x})\mathbf{y} = C_1'\mathbf{m}(k) + C_1''\hat{\mathbf{m}}(k),$$

where $\mathbf{m}(k) = (m_1(\mathbf{x},\mathbf{y}), \ldots, m_k(\mathbf{x},\mathbf{y}))^T$ and $\hat{\mathbf{m}}(k) = (m_{k+1}(k), \ldots, m_n(\mathbf{x},\mathbf{y}))^T$. We can rewrite the last identity as

$$\mathbf{m}(k) = (C_1')^{-1}A_1(\mathbf{x})\mathbf{y} - (C_1')^{-1}C_1''\hat{\mathbf{m}}(k).$$

We now partition C_2 as $C_2 = (C_2'|C_2'')$, where C_2' consists of the first k columns of C_2, and C_2' consists of the last $n-k$ columns. The identity $A_2(\mathbf{x})\mathbf{y} = C_2\mathbf{m}$ can now be written as

$$\begin{aligned} A_2(\mathbf{x})\mathbf{y} &= C_2'\mathbf{m}(k) + C_2\hat{\mathbf{m}}(k) \\ &= C_2'(C_1')^{-1}A_1(\mathbf{x})\mathbf{y} + \left[C_2'' - C_2'(C_1')^{-1}C_1''\right]\hat{\mathbf{m}}(k) \\ &= MA_1(\mathbf{x})\mathbf{y} + N\hat{\mathbf{m}}(k), \end{aligned}$$

where $M = C_2'(C_1')^{-1}$ and $N = C_2'' - C_2'(C_1')^{-1}C_1''$. This last identity can be

rewritten as

$$[A_2(\mathbf{x}) - MA_1(\mathbf{x})]\mathbf{y} = N\hat{\mathbf{m}}(k).$$

So we define a new system of bilinear forms $\mathscr{B}' = A'(\mathbf{x})\mathbf{y} = [A_2(\mathbf{x}) - MA_1(\mathbf{x})]\mathbf{y}$. The system $\mathscr{B}'$ can be computed by the algorithm $\hat{\mathscr{A}} = (m_{k+1}(\mathbf{x},\mathbf{y}),\ldots, m_n(\mathbf{x},\mathbf{y}))$, and therefore $\bar{\mu}(\mathscr{B}') \leqslant \mu(\mathscr{A}) - k$.

We note, again, that $\mathscr{B}'$ is specified not only by $\mathscr{B}$ and $\{B_1,\ldots, B_k\}$, but also by $\mathscr{A}$ and the particular k linearly independent columns of C which were chosen.

We say that $\mathscr{B}'$ is the system obtained by removing $\{B_1,\ldots, B_k\}$ from $\mathscr{B}$, and $m_1(\mathbf{x},\mathbf{y}),\ldots, m_k(\mathbf{x},\mathbf{y})$ are the substituted m/d steps of $\mathscr{A}$.

The construction which was described above shows that $\bar{\mu}(\mathscr{A}) = n \geqslant k$. This is a special case of the row rank theorem, which we will now state.

THEOREM (Row rank). *Let $\mathscr{B} = A(\mathbf{x})\mathbf{y}$ be a system of bilinear forms, and let $r_1(\mathbf{x}),\ldots, r_t(\mathbf{x})$ be the rows of $A(\mathbf{x})$. Then*

$$\bar{\mu}(A(\mathbf{x})\mathbf{y}) \geqslant \dim \mathscr{L}_G(\{r_1(\mathbf{x}),\ldots, r_t(\mathbf{x})\}).$$

III. DEFINITE BILINEAR FORMS

In this section we will prove two theorems about $\bar{\mu}(D(\mathbf{x})\mathbf{y} \oplus A(\boldsymbol{\xi})\boldsymbol{\eta})$, where $D(\mathbf{x})\mathbf{y}$ is a definite system of bilinear forms (definition follows), and $A(\boldsymbol{\xi})\boldsymbol{\eta}$ is an arbitrary system of bilinear forms. For the rest of this section, we let $D(\mathbf{x})\mathbf{y}$ be a system of bilinear forms, where $D(\mathbf{x})$ is a $t \times s$ matrix of linear forms.

Following [7] we define:

DEFINITION 3.1. The system of bilinear forms $D(\mathbf{x})\mathbf{y}$ is called *definite* if for every $0 \neq a \in G^t$ and $0 \neq \mathbf{b} \in G^s$, $\mathbf{a}^T D(\mathbf{x})\mathbf{b} \neq 0$.

It can be easily verified that if $D(\mathbf{x})\mathbf{y}$ is definite then $\bar{\mu}(D(\mathbf{x})\mathbf{y}) \geqslant s + t - 1$.

LEMMA 3.1. *Let $\mathscr{B}$ be the system of bilinear forms*

$$\mathscr{B} = \begin{pmatrix} D(\mathbf{x}) & 0 \\ A'(\mathbf{x}) & A(\boldsymbol{\xi}) \end{pmatrix} \begin{pmatrix} \mathbf{y} \\ \boldsymbol{\eta} \end{pmatrix},$$

where $D(\mathbf{x})\mathbf{y}$ is definite. If $\mathscr{A}$ is an algorithm for computing $\mathscr{B}$ and $\mathscr{A}$ mixes $\mathbf{y}$ and $\boldsymbol{\eta}$, then $\bar{\mu}(\mathscr{A}) \geqslant \bar{\mu}(A(\boldsymbol{\xi})\boldsymbol{\eta}) + s + t$.

Proof. Let $\mathscr{A} = (m_1(\mathbf{x}, \boldsymbol{\xi}; \mathbf{y}, \boldsymbol{\eta}), \ldots, m_n(\mathbf{x}, \boldsymbol{\xi}; \mathbf{y}, \boldsymbol{\eta}))$, where $m_i(\mathbf{x}, \boldsymbol{\xi}; \mathbf{y}, \boldsymbol{\eta}) = L_i(\mathbf{x}, \boldsymbol{\xi}) L_i'(\mathbf{y}, \boldsymbol{\eta})$, $1 \leqslant i \leqslant n$. By assumption, there exists an $L_i'(\mathbf{y}, \boldsymbol{\eta})$ which depends on some $\{y_i\}$ and on some $\{\eta_j\}$. With no loss of generality we will assume that $L_i'(\mathbf{y}, \boldsymbol{\eta}) = \sum_{j=1}^{s} a_{ij} y_j + \sum_{j=1}^{s'} \alpha_{i,j} \eta_j$ with $a_{i,1} \neq 0$ and $\alpha_{i,1} \neq 0$. Because $D(\mathbf{x})\mathbf{y}$ is definite, the system $\mathscr{B}$ depends on $\{y_1, y_2, \ldots, y_s\}$, and therefore $\mathscr{A}$ depends on $\{y_1, \ldots, y_s\}$ as well. That means that there are s $L_i'(\mathbf{y}, \boldsymbol{\eta})$'s which depend on $\{y_1, \ldots, y_s\}$, and we can take $L_i'(\mathbf{y}, \boldsymbol{\eta})$ as one of them. With no loss of generality we may assume that $\{L_i'(\mathbf{y}, \boldsymbol{\eta}) | i = 1, 2, \ldots, s\}$ depend on $\{y_1, \ldots, y_s\}$. We now substitute for $\{y_1, \ldots, y_s\}$, and denote by $\mathscr{B}'$ the system obtained by removing $y_1, \ldots, y_s$ using $L_i'(\mathbf{y}, \boldsymbol{\eta})$, $i = 1, 2, \ldots, s$. The system $\mathscr{B}'$ is

$$\mathscr{B}' = \begin{pmatrix} D(\mathbf{x})M \\ A(\boldsymbol{\xi}) + A'(\mathbf{x})M \end{pmatrix}(\boldsymbol{\eta}),$$

where M is some $s \times s'$ G-matrix. The system $\mathscr{B}'$ satisfies $\bar{\mu}(\mathscr{B}') \leqslant n - s$.

Because we assume that $\alpha_{1,1} \neq 0$, we have that the first column of M is not identically zero; and because $D(\mathbf{x})\mathbf{y}$ is definite, we have $\mathbf{a}^T D(\mathbf{x})M \neq 0$ for every $0 \neq \mathbf{a} \in G^t$. The last statement means that the t bilinear forms $D(\mathbf{x})M\boldsymbol{\eta}$ are G-linearly independent.

Let $\mathscr{B}''$ be the system obtained from $\mathscr{B}'$ by removing $D(\mathbf{x})M\boldsymbol{\eta}$; then

$$\mathscr{B}'' = \left[A(\boldsymbol{\xi}) + A'(\mathbf{x})M + ND(\mathbf{x})M \right] \boldsymbol{\eta},$$

where N is some $t' \times t$ G-matrix. The system $\mathscr{B}''$ satisfies $\bar{\mu}(\mathscr{B}'') \leqslant \bar{\mu}(\mathscr{B}') - t \leqslant n - s - t$.

We now obtain a fourth system, $\tilde{\mathscr{B}} = A(\boldsymbol{\xi})\boldsymbol{\eta}$, from $\mathscr{B}''$ by setting $x_i = 0$, $i = 1, 2, \ldots, r$. The system $\tilde{\mathscr{B}}$ satisfies

$$\bar{\mu}(\tilde{\mathscr{B}}) = \bar{\mu}(A(\boldsymbol{\xi})\boldsymbol{\eta}) \leqslant \bar{\mu}(\mathscr{B}'') \leqslant n - s - t;$$

that is, $n \geqslant \bar{\mu}(A(\boldsymbol{\xi})\boldsymbol{\eta}) + s + t$. This proves the lemma. ∎

THEOREM 3.1. *Let $D(\mathbf{x})\mathbf{y}$ be definite system of bilinear forms, and let $A(\boldsymbol{\xi})\boldsymbol{\eta}$ be an arbitrary system of bilinear forms. If $\bar{\mu}(D(\mathbf{x})\mathbf{y}) = s + t$ then $\bar{\mu}(D(\mathbf{x})\mathbf{y} \oplus A(\boldsymbol{\xi})\boldsymbol{\eta}) = \bar{\mu}(D(\mathbf{x})\mathbf{y} + \bar{\mu}(A(\boldsymbol{\xi})\boldsymbol{\eta}) = \bar{\mu}(A(\boldsymbol{\xi})\boldsymbol{\eta}) + s + t$. [Recall that we assume that $D(\mathbf{x})$ is a $t \times s$ matrix.]*

Proof. Let $\mathscr{A} = (m_1(\mathbf{x}, \boldsymbol{\xi}; \mathbf{y}, \boldsymbol{\eta}), \ldots, m_n(\mathbf{x}, \boldsymbol{\xi}; \mathbf{y}, \boldsymbol{\eta}))$ be an algorithm which computes $(D(\mathbf{x})\mathbf{y} \oplus A(\boldsymbol{\xi})\boldsymbol{\eta})$. We want to show that $n \geqslant \bar{\mu}(A(\boldsymbol{\xi})\boldsymbol{\eta}) + s + t$. If $\mathscr{A}$ mixes $\mathbf{y}$ and $\boldsymbol{\eta}$, then the result follows from Lemma 3.1. If $\mathscr{A}$ is partitioned

by y and η, then by Lemma 2.2 either $n > \bar{\mu}(A(\xi)\eta) + s + t$ or else $\mathscr{A}$ is a direct sum algorithm, and therefore $n = \bar{\mu}(A(\xi)\eta) + s + t$. In either case the theorem is proved. ∎

COROLLARY 3.1. *Let $\mathscr{B}_Q = \{B_0, B_1, B_2, B_3\}$ be the system of quaternion multiplication, i.e. $B_0 + iB_1 + jB_2 + kB_3 = (x_0 + ix_1 + jx_2 + kx_3)(y_0 + iy_1 + jy_2 + ky_3)$, $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$. Let $A(\xi)\eta$ be an arbitrary system of bilinear forms. If $G \leqslant \mathbb{R}$ is a subfield of the real numbers, then $\bar{\mu}(\mathscr{B}_Q \oplus A(\xi)\eta) = \bar{\mu}(A(\xi)\eta) + \bar{\mu}(\mathscr{B}_Q) = \bar{\mu}(A(\xi)\eta) + 8$.*

Proof. It was cited in [8] that if $G \leqslant \mathbb{R}$ then $\bar{\mu}(\mathscr{B}_Q) = 8$. It is also easily verified that, under the same assumption on G, $\mathscr{B}_Q$ is definite. The corollary now follows from Theorem 3.1. ∎

The assumption that $G \leqslant \mathbb{R}$ was necessary; otherwise $\mathscr{B}_Q$ is not definite. In fact, if G includes the element $\sqrt{-1}$, then $\mathscr{B}_Q$ can be transformed into the system $\langle 2,2,2\rangle$ of the product of two 2×2 matrices. This latter system will be studied in Section V.

THEOREM 3.2. *Let $D(\mathbf{x})\mathbf{y}$ be a definite system of bilinear forms, and let $A(\xi)\eta$ be an arbitrary system of bilinear forms. If $\bar{\mu}(D(\mathbf{x})\mathbf{y}) = s + t - 1$ then $\bar{\mu}(D(\mathbf{x})\mathbf{y} \oplus A(\xi)\eta) = \bar{\mu}(D(\mathbf{x})\mathbf{y}) + \bar{\mu}(A(\xi)\eta)$. Moreover, $D(\mathbf{x})\mathbf{y}$ and $A(\xi)\eta$ satisfy the direct sum conjecture strongly. (Again, $D(\mathbf{x})$ is a $t \times s$ matrix.)*

Proof. Let $\mathscr{A}$ be a minimal algorithm for computing $D(\mathbf{x})\mathbf{y} \oplus A(\xi)\eta$. The algorithm $\mathscr{A}$ satisfies $\bar{\mu}(\mathscr{A}) \leqslant \bar{\mu}(D(\mathbf{x})\mathbf{y}) + \bar{\mu}(A(\xi)\eta) < \bar{\mu}(A(\xi)\eta) + s + t$. By Lemma 3.1, $\mathscr{A}$ is partitioned by y and η, and therefore, by Lemma 2.2, $\mathscr{A}$ is a direct sum algorithm and $\bar{\mu}(\mathscr{A}) = \bar{\mu}(D(\mathbf{x})\mathbf{y}) + \bar{\mu}(A(\xi)\eta)$. This proves the theorem. ∎

Before stating a corollary of this theorem, we should recall some notation which was introduced in Section I. Let $P(u) \in G[u]$ be a monic polynomial, and let $t = \deg(P(u))$. We use $\mathscr{B}(P)$ to denote the system of bilinear forms of the product of polynomials modulo $P(u)$. More precisely, $\mathscr{B}(P) = \{B_0, B_1, \ldots, B_{t-1}\}$, where

$$\sum_{i=0}^{t-1} B_i u^i = \left(\sum_{i=0}^{t-1} x_i u^i\right)\left(\sum_{i=0}^{t-1} y_i u^i\right) \bmod P(u).$$

COROLLARY 3.2. *Let $P(u) \in G[u]$ be an irreducible polynomial of degree t, and let $A(\xi)\eta$ be an arbitrary system of bilinear forms. If $|G| \geqslant 2t - 2$*

then $\bar{\mu}(\mathscr{B}(P)\oplus A(\xi)\eta)=\bar{\mu}(\mathscr{B}(P))+\bar{\mu}(A(\xi)\eta)$. *Moreover,* $\mathscr{B}(P)$ *and* $A(\xi)\eta$ *satisfy the direct sum conjecture strongly.*

Proof. It was shown in [4] that, under the assumption on $P(u)$ and $|G|$, $\bar{\mu}(\mathscr{B}(P))=2t-1$. It is easily verified that, because $P(u)$ is irreducible, $\mathscr{B}(P)$ is definite. The corollary then follows from Theorem 3.2. ■

COROLLARY 3.3. *Let* $P(u)\in G[u]$ *be a product of distinct irreducible polynomials, i.e.* $P(u)=\prod_{i=1}^{k}P_i(u)$, $P_i(u)$ *irreducible,* $1\leqslant i\leqslant k$, *and* $(P_i(u),P_j(u))=1$ *for* $i\neq j$, $1\leqslant i,j\leqslant k$. *If* $|G|\geqslant max_{1\leqslant i\leqslant k}\{2\deg(P_i(u))-2\}$, *then for any system* $A(\xi)\eta$, $\beta(P)$ *and* $A(\xi)\eta$ *satisfy the direct sum conjecture strongly.*

Proof. It was shown in [4] that under the assumption on $|G|$, $\bar{\mu}(\mathscr{B}(P))=\sum_{i=1}^{k}(2t_i-1)$, where $t_i=\deg(P_i(u))$, $1\leqslant i\leqslant k$. By the Chinese Remainder Theorem (see, for example, [9]), $\mathscr{B}(P)$ is equivalent to $\mathscr{B}(P_1)\oplus\mathscr{B}(P_2)\oplus\cdots\oplus\mathscr{B}(P_k)$. Repeated use of Corollary 3.2 yields the desired result. ■

The more general case of $\mathscr{B}(P)$, where $P(u)$ is allowed to have, as a factor, a power of an irreducible polynomial, will be discussed in the next section.

IV. DIRECT SUM OF $\mathscr{B}(P)$

The purpose of this section is to extend the result of Corollary 3.2 to the case $P=Q^l$, where Q is an irreducible polynomial. In the case that $l\geqslant 2$, the system $\mathscr{B}(P)$ is not definite, so Theorems 3.1 and 3.2 cannot be used directly. We will first investigate how "far" $\mathscr{B}(P)$ is from being definite, and then prove the main result of the section.

Let $\mathscr{B}(P)=R(\mathbf{x})\mathbf{y}$, where $R(\mathbf{x})$ is a $t\times t$ matrix. There exist $\mathbf{a},\mathbf{b}\in G^t$ such that $\mathbf{a}^tR(\mathbf{x})\mathbf{b}=0$ even though $\mathbf{a}\neq 0$ and $\mathbf{b}\neq 0$. Before we prove the theorem we will determine the set $I\subseteq G^t\times G^t$, where $I=\{(\mathbf{a},\mathbf{b})|\mathbf{a}^TR(\mathbf{x})\mathbf{b}=0\}$. A convenient language for describing the set I is that of the zero divisors of the algebra $G[u]/\langle P(u)\rangle$.

Let $P(u)=u^t+\sum_{i=0}^{t-1}\alpha_iu^i$ be a polynomial. We will use C to denote the companion matrix of P, that is,

$$C=\begin{pmatrix}0&0&0&-\alpha_0\\1&0&0&-\alpha_1\\0&1&0&-\alpha_2\\\vdots&\vdots&\vdots&\vdots\\0&0&1&-\alpha_{t-1}\end{pmatrix}.$$

[It would have been more accurate to denote the companion matrix by $C(P)$, to indicate its dependence on the polynomial $P(u)$. But as $P(u)$ will be fixed during the discussion, we have opted for the simpler notation.]

Now, if $\mathscr{B}(P) = R(\mathbf{x})\mathbf{y}$ then $R(\mathbf{x}) = \sum_{i=0}^{t-1} x_i C^i$. But multiplication of polynomials is commutative, and therefore $(\sum_{i=0}^{t-1} x_i C^i)\mathbf{y} = (\sum_{i=0}^{t-1} y_i C^i)\mathbf{x}$. Let $\mathbf{b} = (b_0, b_1, \ldots, b_{t-1})^T$; then $R(\mathbf{x})\mathbf{b} = (\sum_{i=0}^{t-1} x_i C^i)\mathbf{b} = (\sum_{i=0}^{t-1} b_i C^i)\mathbf{x}$. Therefore, if $\mathbf{a}^T R(\mathbf{x})\mathbf{b} = 0$, then $\mathbf{a}^T(\sum_{i=0}^{t-1} b_i C^i)\mathbf{x} = 0$, which means that $\mathbf{a}^T$ is a (left) annihilator of the G-matrix $R(\mathbf{b}) = \sum_{i=0}^{t-1} b_i C^i$.

Because every matrix is similar to its transpose, we can write

$$C = KC^T K^{-1}$$

for some nonsingular matrix K. Thus $R(\mathbf{b}) = K[\sum_{i=0}^{t-1} b_i (C^T)^i]K^{-1} = KR(\mathbf{b})^T K^{-1}$. If we now let $\mathbf{a} = (a_0, a_1, \ldots, a_{t-1})^T$ and $\mathbf{a}' = K^T\mathbf{a} = (a'_0, a'_1, \ldots, a'_{t-1})^T$, then $\mathbf{a}^T R(\mathbf{x})\mathbf{b} = 0$ if and only if $0 = \mathbf{a}^T R(\mathbf{b}) = \mathbf{a}^T K R(\mathbf{b})^T K^{-1} = (\mathbf{a}')^T R(\mathbf{b})^T K^{-1}$. But K is nonsingular, so the condition means that $(\mathbf{a}')^T R(\mathbf{b})^T = 0$, or $R(\mathbf{b})\mathbf{a}' = 0$. (In this paragraph we have used 0 with three different meanings: the scalar 0, the zero row vector, and the zero column vector. But as the meaning is clear in each use, we trust that no confusion resulted.) The vector $\mathbf{c} = R(\mathbf{b})\mathbf{a}'$, where $\mathbf{c} = (c_0, c_1, \ldots, c_{t-1})^T$, can be expressed as coefficients of a polynomial; namely,

$$\sum_{i=0}^{t-1} c_i u^i = \left(\sum_{i=0}^{t-1} a'_i u^i\right)\left(\sum_{i=0}^{t-1} b_i u^i\right) \bmod P(u).$$

We will summarize this discussion by:

LEMMA 4.1. $\mathbf{a}^T R(\mathbf{x})\mathbf{b} = 0$ *if and only if* $0 = (\sum_{i=0}^{t-1} a'_i u^i)(\sum_{i=0}^{t-1} b_i u^i) \bmod P(u)$, *where* $\mathbf{a}' = K^T\mathbf{a}$.

It will be convenient, later in the section, to have an equivalent form of Lemma 4.1, namely:

LEMMA 4.2. $\mathbf{a}^T K^{-1} R(\mathbf{x})\mathbf{b} = 0$ *if and only if* $0 = (\sum_{i=0}^{t-1} a_i u^i)(\sum_{i=0}^{t-1} b_i u^i) \bmod P(u)$.

As was mentioned at the beginning of the section, we assume that $P(u) = Q(u)^l$, where $Q(u)$ is an irreducible polynomial. In this case, if $0 = (\sum_{i=0}^{t-1} a_i u^i)(\sum_{i=0}^{t-1} b_i u^i) \bmod P(u)$, then both polynomials $0 \neq \sum_{i=0}^{t-1} a_i u^i$ and $0 \neq \sum_{i=0}^{t-1} b_i u^i$ are divisible by $Q(u)$. In other words, if the polynomial $\sum_{i=0}^{t-1} a_i u^i$ is not divisible by $Q(u)$, then $\mathbf{a}^T K^{-1} R(\mathbf{x})\mathbf{b} = 0$ implies that $\mathbf{b} = 0$. This last sentence can be paraphrased as:

LEMMA 4.3. *If* $\sum_{i=0}^{t-1} a_i u^i$ *is not divisible by* $Q(u)$, *then the bilinear form* $[\mathbf{a}^T K^{-1} R(\mathbf{x})]\mathbf{y}$ *is definite, and therefore* $\bar{\mu}([\mathbf{a}^T K^{-1} R(\mathbf{x})]\mathbf{y}) = t$.

Let us denote the degree of $Q(u)$ by $s = t/l$. We can write the polynomial $\sum_{i=0}^{t-1} a_i u^i$ as $\sum_{i=0}^{t-1} a_i u^i = \sum_{i=0}^{s-1} \bar{a}_i u^i + Q(u) \sum_{i=s}^{t-s-1} \tilde{a}_i u^{s-i}$. The advantage of this terminology is that $\sum_{i=0}^{t-1} a_i u^i$ is not divisible by $Q(u)$ if and only if $\tilde{a}_i \neq 0$ for some $i = 0, 1, \ldots, s-1$. If we are presented with a polynomial $\sum_{i=0}^{s-1} \tilde{a}_i u^i + Q(u) \sum_{i=s}^{t-s-1} \tilde{a}_i u^{s-i} = \sum_{i=0}^{t-1} a_i u^i$, then $\mathbf{a}^T = \tilde{\mathbf{a}}^T U$ for some nonsingular G-matrix U, where $\tilde{\mathbf{a}}^T = (\tilde{a}_0, \ldots, \tilde{a}_{t-1})$. We can now restate Lemma 4.3, replacing $\tilde{\mathbf{a}}$ by $\mathbf{a}$, as:

LEMMA 4.4. *If* $a_i \neq 0$ *for some* $i = 0, 1, \ldots, s-1$, *then the bilinear form* $[\mathbf{a}^T U K^{-1} R(\mathbf{x})]\mathbf{y}$ *is definite, and therefore* $\bar{\mu}([\mathbf{a}^T U K^{-1} R(\mathbf{x})]\mathbf{y}) = t$.

The main result of this section, which we will state and prove shortly, is that for any system of bilinear forms $A'(\boldsymbol{\xi})\boldsymbol{\eta}$, $\mathscr{B}(P)$ and $A'(\boldsymbol{\xi})\boldsymbol{\eta}$ satisfy the direct sum conjecture strongly, whenever $P(u) = Q(u)^l$ and $Q(u)$ is irreducible. Lemma 4.4 suggest that it is more convenient to consider the system $UK^{-1}R(\mathbf{x})\mathbf{y}$ instead of $\mathscr{B}(P) = R(\mathbf{x})\mathbf{y}$. The next lemma shows that these two systems are equivalent.

LEMMA 4.5. *Let* V *be a* $t \times t$ *nonsingular* G*-matrix.* $A(\mathbf{x})\mathbf{y}$ *and* $A'(\boldsymbol{\xi})\boldsymbol{\eta}$ *satisfy the direct sum conjecture (strongly) if and only if* $VA(\mathbf{x})\mathbf{y}$ *and* $A'(\boldsymbol{\xi})\boldsymbol{\eta}$ *do.*

Proof. Let $\mathscr{A} = (m_1(\mathbf{x}, \boldsymbol{\xi}; \mathbf{y}, \boldsymbol{\eta}), \ldots, m_n(\mathbf{x}, \boldsymbol{\xi}; \mathbf{y}, \boldsymbol{\eta}))$ be an algorithm which computes $A(\mathbf{x})\mathbf{y} \oplus A'(\boldsymbol{\xi})\boldsymbol{\eta}$. That means that

$$\begin{pmatrix} A(\mathbf{x}) & 0 \\ 0 & A'(\boldsymbol{\xi}) \end{pmatrix} \begin{pmatrix} \mathbf{y} \\ \boldsymbol{\eta} \end{pmatrix} = \hat{C}\mathbf{m} = \begin{pmatrix} \hat{C}_1 \\ \hat{C}_2 \end{pmatrix} \mathbf{m}$$

and therefore

$$\begin{pmatrix} VA(\mathbf{x}) & 0 \\ 0 & A'(\boldsymbol{\xi}) \end{pmatrix} \begin{pmatrix} \mathbf{y} \\ \boldsymbol{\eta} \end{pmatrix} = \begin{pmatrix} V\hat{C}_1 \\ \hat{C}_2 \end{pmatrix} \mathbf{m}.$$

That is, every algorithm for computing $A(\mathbf{x})\mathbf{y} \oplus A'(\boldsymbol{\xi})\boldsymbol{\eta}$ can also be used to compute $VA(\mathbf{x})\mathbf{y} \oplus A'(\boldsymbol{\xi})\boldsymbol{\eta}$. The converse is obtained by the nonsingularity of V. ∎

THEOREM 4.1. *Let* $Q(u)^l = P(u) \in G[u]$ *be a polynomial of degree* t, *where* $Q(u)$ *is irreducible. If* $|G| \geqslant 2t - 2$, *then for any* $A'(\boldsymbol{\xi})\boldsymbol{\eta}$, $\mathscr{B}(P)$ *and*

$A'(\xi)\eta$ satisfy the direct sum conjecture strongly. That is, $\bar{\mu}(\mathscr{B}(P)\oplus A'(\xi)\eta) = \bar{\mu}(\mathscr{B}(P))+\bar{\mu}(A'(\xi)\eta)$, and every minimal algorithm for computing $\mathscr{B}(P)\oplus A'(\xi)\eta$ is a direct sum algorithm.

Proof. It was shown in [4] that if $|G| \geqslant 2t-2$ then $\bar{\mu}(\mathscr{B}(P)) = 2t-1$. Let $\mathscr{A} = (m_1(\mathbf{x}, \xi; \mathbf{y}, \eta), \ldots, m_n(\mathbf{x}, \xi; \mathbf{y}, \eta))$ be a minimal algorithm for computing $\mathscr{B}(P)\oplus A'(\xi)\eta = R(\mathbf{x})\mathbf{y}\oplus A'(\xi)\eta$. We of course have $n \leqslant \bar{\mu}(R(\mathbf{x})\mathbf{y})+\bar{\mu}(A'(\xi)\eta) = \bar{\mu}(A'(\xi)\eta)+2t-1$. By Lemma 4.5 we can replace $R(\mathbf{x})\mathbf{y}$ by $UK^{-1}R(\mathbf{x})\mathbf{y}$, where U and K are as in Lemma 4.4. The proof of Lemma 4.4 shows that $\mathscr{A}$ can compute $UK^{-1}R(\mathbf{x})\mathbf{y}\oplus A'(\xi)\eta$ as well. Let $(B_0, B_1, \ldots, B_{t-1})$ be the bilinear forms $UK^{-1}R(\mathbf{x})\mathbf{y}$; then $B_1, B_2, \ldots, B_{t-1}$ are G-linearly independent. Let $\mathscr{B}'$ be the system of bilinear forms obtained from $UK^{-1}R(\mathbf{x})\mathbf{y}\oplus A'(\xi)\eta$ by removing $B_1, B_2, \ldots, B_{t-1}$, and let $m_1(\mathbf{x}, \xi; \mathbf{y}, \eta), \ldots, m_{t-1}(\mathbf{x}, \xi; \mathbf{y}, \eta)$ be the substituted m/d steps of $\mathscr{A}$.

The system $\mathscr{B}'$ can be written as

$$\mathscr{B}' = \begin{pmatrix} \mathbf{a}^T UK^{-1}R(\mathbf{x}) & 0 \\ MR'(\mathbf{x}) & A'(\xi) \end{pmatrix} \begin{pmatrix} \mathbf{y} \\ \eta \end{pmatrix},$$

where $\mathbf{a} \in G^t$ satisfies $a_1 = 1$, $R'(\mathbf{x})$ is the matrix of the last $t-1$ rows of $UK^{-1}R(\mathbf{x})$, and M is some $t' \times (t-1)$ G-matrix.

The system $\mathscr{B}'$ satisfies $\bar{\mu}(\mathscr{B}') \leqslant n-(t-1) \leqslant \bar{\mu}(A'(\xi)\eta)+t$. In fact, the algorithm $\mathscr{A}' = (m_t(\mathbf{x}, \xi; \mathbf{y}, \eta), \ldots, m_n(\mathbf{x}, \xi; \mathbf{y}, \eta))$ can compute $\mathscr{B}'$. By Lemma 4.4, $\mathbf{a}^T UK^{-1}R(\mathbf{x})\mathbf{y}$ is definite, and by Lemma 3.1, $\mathscr{A}'$ is partitioned by $\mathbf{y}$ and η. If we now set all the y_i's to be 0, we obtain from $\mathscr{A}'$ an algorithm which computes $A'(\xi)\mathbf{y}$, and therefore there are at least $n' = \bar{\mu}(A'(\xi)\eta)m_i(\mathbf{x}, \xi; \mathbf{y}, \eta) = L_i(\mathbf{x}, \xi)L_i'(\mathbf{y}, \eta)$ such that $L_i'(\mathbf{y}, \eta)$ does not depend on any y_i. [Recall that each $L_i'(\mathbf{y}, \eta)$, $t \leqslant i \leqslant n$, depends either on some y_j or on some η_j but not on both.] Similarly, if we set all the η_j's to be 0, we obtain from $\mathscr{A}'$ an algorithm which computes

$$\overline{\mathscr{B}} = \begin{pmatrix} \mathbf{a}^T UK^{-1}R(\mathbf{x}) \\ MR'(\mathbf{x}) \end{pmatrix} \mathbf{y},$$

and therefore at least $n'' = \bar{\mu}(\overline{\mathscr{B}}) \geqslant \bar{\mu}(a^T UK^{-1}R(\mathbf{x})\mathbf{y}) = t$ $L_i'(\mathbf{y}, \eta)$'s which depend on some y_j but not on any η_j. However, $n'+t = \bar{\mu}(A'(\xi)\eta)+t \geqslant n-t+1 \geqslant n'+n'' \geqslant n'+t$. Therefore $n'' = t$, and $n \geqslant \bar{\mu}(A'(\xi)\eta)+2t-1$. In other words $\mathscr{B}(P)$ and $A'(\xi)\eta$ satisfy the direct sum conjecture.

To show that $\mathscr{B}(P)$ and $A'(\xi)\eta$ satisfy the direct sum conjecture strongly, we assume, with no loss of generality, that $L_i'(\mathbf{y}, \eta)$, $t \leqslant i \leqslant 2t-1$, does not

depend on any η_j, and $L_i'(\mathbf{y}, \boldsymbol{\eta})$, $2t \leqslant i \leqslant n$, does not depend on any y_j. Because the algorithm $\mathscr{A}$ computes $R(\mathbf{x})\mathbf{y} \oplus A'(\boldsymbol{\xi})\boldsymbol{\eta}$, the algorithm $\mathscr{A}''$, obtained from $\mathscr{A}$ by setting all the η_j's to be 0, computes $R(\mathbf{x})\mathbf{y}$. Similarly, the algorithm $\mathscr{A}'''$, obtained from $\mathscr{A}$ by setting all the y_j's to be 0, computes $A'(\boldsymbol{\xi})\boldsymbol{\eta}$.

Now, $\mathscr{A}'' = (m_1'(\mathbf{x}, \boldsymbol{\xi}; \mathbf{y}), \ldots, m_{2t-1}(\mathbf{x}, \boldsymbol{\xi}; \mathbf{y}))$, where $m_i'(\mathbf{x}, \boldsymbol{\xi}; \mathbf{y}) = L_i(\mathbf{x}, \boldsymbol{\xi}) L_i'(\mathbf{y}, \boldsymbol{\eta} = 0)$, $1 \leqslant i \leqslant 2t - 1$, is a minimal algorithm for $R(\mathbf{x})\mathbf{y}$, and by Lemma 2.1 $L_i(\mathbf{x}, \boldsymbol{\xi})$, $1 \leqslant i \leqslant 2t - 1$, does not depends on any ξ_j. That means that $\mathscr{A}$ is partitioned by $\mathbf{x}$ and $\boldsymbol{\xi}$, and by Lemma 2.2 $\mathscr{A}$ is a direct sum algorithm. This proves the theorem. ■

Just as in the proof of Corollary 3.3, the Chinese Remainder Theorem and repeated use of Theorem 4.1 yield:

COROLLARY 4.1. *Let* $P(u) = \prod_{i=1}^{k} Q_i(u)^{l_i}$, *where* $Q_i(u)$ *is irreducible, and* $(Q_i(u), Q_j(u)) = 1$, $1 \leqslant i, j \leqslant k$, $i \neq j$. *If* $|G| \geqslant \max\{2l_i \deg Q_i(u) - 2\}$, *then* $A'(\boldsymbol{\xi})\boldsymbol{\eta}$ *and* $\mathscr{B}(P)$ *satisfy the direct sum conjecture strongly, for every system* $A'(\boldsymbol{\xi})\boldsymbol{\eta}$.

We have recently become aware of a result which generalizes our last corollary [11]. It says that a direct sum of local algebras of minimal rank satisfies the direct sum conjecture strongly.

V. DIRECT SUM OF $\langle 2,2,2 \rangle$

The main result of this section is that $\langle 2,2,2 \rangle$ and $A'(\boldsymbol{\xi})\boldsymbol{\eta}$ satisfy the direct sum conjecture strongly, where, as in Section I, $\langle 2,2,2 \rangle$ denotes the system $\{B_{ik} \mid 1 \leqslant i, k \leqslant 2\}$, and $B_{ik} = \sum_{j=1}^{2} x_{ij} y_{jk}$. The proof of the main result will necessitate the study of bilinear forms given by

$$\tilde{\mathscr{B}} = \begin{pmatrix} B_1 & B_3 \\ B_2 & B_4 \end{pmatrix} = \begin{pmatrix} u_1 & u_3 \\ u_2 & u_4 \end{pmatrix} \begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix}$$

where $u_i = u_i(\mathbf{x}; \boldsymbol{\xi})$ is a linear form of the indeterminates $\mathbf{x}$ and $\boldsymbol{\xi}$, $1 \leqslant i \leqslant 4$, and the y_j's are indeterminates. We will first state, and prove, several lemmas about $\tilde{\mathscr{B}}$, and then state and prove the main result.

If $\dim L_G(u_1, u_2, u_3, u_4) = 4$, then by linear change of variables the system $\tilde{\mathscr{B}}$ can be transformed to $\langle 2,2,2 \rangle$. We will therefore concentrate on the case that $\dim L_G(u_1, u_2, u_3, u_4) = 3$. With no loss of generality, we may assume that $\{u_1, u_2, u_3\}$ are G-linearly independent, and $u_4 = \alpha u_1 + \beta u_2 + \gamma u_3$.

Let us, first, transform $\tilde{\mathscr{B}}$ to an equivalent system $\hat{\mathscr{B}}$ given by

$$\hat{\mathscr{B}} = \left[\begin{pmatrix} 1 & 0 \\ -\gamma & 1 \end{pmatrix}\begin{pmatrix} u_1 & u_3 \\ u_2 & u_4 \end{pmatrix}\begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix}\right] \times \left[\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix}\right]$$

$$= \begin{pmatrix} u_1 & u_3 - \beta u_1 \\ u_2 - \gamma u_1 & (\alpha + \beta\gamma)u_1 \end{pmatrix}\begin{pmatrix} y_1 + \beta y_2 & y_3 + \beta y_4 \\ y_2 & y_4 \end{pmatrix}.$$

The linear forms $u_1, u_2 - \gamma u_1, u_3 - \beta u_1$ are still G-linearly independent; the fourth term, $(\alpha + \beta\gamma)u_1$, may vanish or may be a nonzero multiple of u_1. In the first case, a suitable change of variables transforms $\hat{\mathscr{B}}$ (and therefore $\tilde{\mathscr{B}}$) into

$$\begin{pmatrix} x_1 & x_3 \\ x_2 & 0 \end{pmatrix}\begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix}.$$

In the second case, a suitable change of variables transforms $\hat{\mathscr{B}}$ (and $\tilde{\mathscr{B}}$) into

$$\begin{pmatrix} x_1 & x_3 \\ x_2 & x_1 \end{pmatrix}\begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix}.$$

We will deal with the second case first, and then turn our attention to the first case.

One way of characterizing the two cases is by the definiteness of matrix

$$U = \begin{pmatrix} u_1 & u_3 \\ u_2 & u_4 \end{pmatrix}.$$

The first case is equivalent to saying that there exist two nonzero vectors $\mathbf{a}, \mathbf{b} \in G^2$ such that $\mathbf{a}^T U \mathbf{b} = 0$, while the second case is equivalent to saying that $\mathbf{a}^T U \mathbf{b} = 0$ implies $\mathbf{a} = 0$ or $\mathbf{b} = 0$.

LEMMA 5.1. *Let $\tilde{\mathscr{B}}$ be the system of bilinear forms*

$$\begin{pmatrix} B_1 & B_3 \\ B_2 & B_4 \end{pmatrix} = \begin{pmatrix} x_1 & x_3 \\ x_2 & x_1 \end{pmatrix}\begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix}.$$

Then $\bar{\mu}(\tilde{\mathscr{B}}) = 6$.

Proof. Let us write $\tilde{\mathscr{B}}$ as $A(\mathbf{x})\mathbf{y}$, that is,

$$\tilde{\mathscr{B}} = \begin{pmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \end{pmatrix} = \begin{pmatrix} x_1 & x_3 & 0 & 0 \\ x_2 & x_1 & 0 & 0 \\ 0 & 0 & x_1 & x_3 \\ 0 & 0 & x_2 & x_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}.$$

Let $\mathscr{A}$ be a minimal algorithm for computing $\tilde{\mathscr{B}}$. Because B_1 and B_3 are G-linearly independent, we can substitute for them, resulting in the system

$$\mathscr{B}' = \begin{pmatrix} B_2' \\ B_4' \end{pmatrix} = \begin{pmatrix} x_2 + ax_1 & x_1 + ax_3 & bx_1 & bx_3 \\ cx_1 & cx_3 & x_2 + dx_1 & x_1 + dx_3 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = A'(\mathbf{x})\mathbf{y}$$

satisfying $\bar{\mu}(\mathscr{B}') \leqslant \bar{\mu}(\tilde{\mathscr{B}}) - 2$. We will now show that the four columns of $A'(\mathbf{x})$ are G-linearly independent; and therefore, by the column rank theorem, $\bar{\mu}(\mathscr{B}') \geqslant 4$, which implies that $\bar{\mu}(\tilde{\mathscr{B}}) \geqslant 6$.

Assume that

$$\begin{pmatrix} x_2 + ax_1 & x_1 + ax_3 & bx_1 & bx_3 \\ cx_1 & cx_3 & x_2 + dx_1 & x_1 + dx_3 \end{pmatrix} \begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

In the first row of $A'(\mathbf{x})$ we have x_2 appearing only in the first column, so $g_1 = 0$. Similarly $g_3 = 0$. Once we know that $g_1 = g_3 = 0$, we see that x_1 can vanish in the first row only if $g_2 = 0$, and x_1 can vanish in the second row only if $g_4 = 0$.

To finish the proof of lemma we observe that

$$\begin{pmatrix} x_1 & x_3 \\ x_2 & x_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1(y_1 + y_2) + (x_3 - x_1)y_2 \\ x_1(y_1 + y_2) + (x_2 - x_1)y_1 \end{pmatrix},$$

and therefore $\bar{\mu}(\tilde{\mathscr{B}}) \leqslant 6$. ∎

We will now assume that $u_1 = x_1$, $u_2 = x_2$, $u_3 = u_3(x_1, x_2; \xi)$, $u_4 = u_4(x_1, x_2; \xi)$, where either u_3 or u_4 depends on some ξ_i. No assumption is made on the dependence of u_3 and u_4 on x_1 and x_2. The next lemma shows that we can assume that u_3 and u_4 depend on $\{x_1, x_2\}$.

LEMMA 5.2. *Let*

$$U = \begin{pmatrix} x_1 & u_3(x_1, x_2; \xi) \\ x_2 & u_4(x_1, x_2; \xi) \end{pmatrix},$$

and let $\mathscr{B}$ *be the system*

$$\mathscr{B} = U\begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix}.$$

If $|G| \geqslant 3$, *there exists a system*

$$\mathscr{B}' = U'\begin{pmatrix} y_1 & y_4 \\ y_2 & y_4 \end{pmatrix},$$

equivalent to $\mathscr{B}$, *such that*

$$U' = \begin{pmatrix} x_1 & u_3'(x_1, x_2; \xi) \\ x_2 & u_4'(x_1, x_2; \xi) \end{pmatrix}$$

and u_3', u_4' *depend on* $\{x_1, x_2\}$.

Proof. For any $g \in G$ the system

$$\mathscr{B}' = U\begin{pmatrix} y_1 + gy_2 & y_3 + gy_4 \\ y_2 & y_4 \end{pmatrix}$$

is equivalent to $\mathscr{B}$. But $\mathscr{B}'$ can be written as

$$U'\begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix}, \qquad \text{where} \quad U' = \begin{pmatrix} x_1 & u_3' \\ x_2 & u_4' \end{pmatrix}$$

and $u_3' = u_3 + gx_1$, $u_4' = u_4 + gx_2$. Let us write u_3 and u_4 as

$$\begin{pmatrix} u_3 \\ u_4 \end{pmatrix} = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} L_1(\xi) \\ L_2(\xi) \end{pmatrix} = M\mathbf{x} + \mathbf{L}(\xi);$$

then u_3' and u_4' can be written as

$$\begin{pmatrix} u_3' \\ u_4' \end{pmatrix} = (M + gI)\mathbf{x} + \mathbf{L}(\xi).$$

If $|G| \geqslant 3$, there exists a $g \in G$ such that $M + gI$ is nonsingular. This proves the lemma. ■

In the next lemma we will assume that

$$U' = \begin{pmatrix} x_1 & u_3(x_1, x_2; \xi) \\ x_2 & u_4(x_1, x_2; \xi) \end{pmatrix}$$

is definite and that either u_3 or u_4 depends on some ξ_i; i.e., $\dim L_G(x_1, x_2, u_3, u_4) \geqslant 3$. We will denote by $\tilde{\mathscr{B}}$ the system

$$\tilde{\mathscr{B}} = U \begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix}$$

and by $\mathscr{B}$ the system

$$\mathscr{B} = \begin{pmatrix} U & 0 & 0 \\ 0 & U & 0 \\ 0 & 0 & A'(\xi) \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ \eta \end{pmatrix}.$$

(Note that because U depends on ξ, $\mathscr{B}$ is not a direct sum.)

LEMMA 5.3. *Let $\mathscr{B}$ be as above. If $|G| \geqslant 3$ then $\bar{\mu}(\mathscr{B}) \geqslant \bar{\mu}(A'(\xi)\eta) + 6$.*

Proof. Let $\mathscr{A} = (m_1(\mathbf{x}, \xi; \mathbf{y}, \eta), \ldots, m_n(\mathbf{x}, \xi; \mathbf{y}, \eta))$ be a minimal algorithm for $\mathscr{B}$, where $m_i(\mathbf{x}, \xi; \mathbf{y}, \eta) = L_i(\mathbf{x}, \xi) L_i'(\xi, \eta)$, $1 \leqslant i \leqslant n$. If $\mathscr{A}$ is partitioned by y and η, then there are at least $n' = \bar{\mu}(A'(\xi)\eta)$ $L_i'(\mathbf{y}, \eta)$'s which depend on some η_i but not on a y_j, and, by Lemma 5.1, at least 6 $L_i'(\mathbf{y}, \eta)$'s which depend on some y_i but not on an η_j. But $n \geqslant n' + 6$, which proves the lemma in this case.

We will assume now that $\mathscr{A}$ mixes y and η. By Lemma 5.2, we also assume that u_3, u_4 depend on $\{x_1, x_2\}$. With no loss of generality, we assume

that $L_1'(\mathrm{y}, \eta)$ depends on, say, y_2 and on, say, η_1. Because $\mathscr{B}$ depends on $\{y_2, y_4\}$, we assume that $L_1'(\mathrm{y}, \eta)$ and $L_2'(\mathrm{y}, \eta)$ depend on $\{y_2, y_4\}$. [Note that we do not assume that $L_2'(\mathrm{y}, \eta)$ depends on an η_j.] Substituting for $\{y_2, y_4\}$ in $L_1'(\mathrm{y}, \eta)$ and $L_2'(\mathrm{y}, \eta)$, we transform $\mathscr{B}$ into

$$\mathscr{B}' = \begin{pmatrix} U_1 & U_2 & A_1 \\ U_3 & U_4 & A_2 \\ 0 & & A'(\xi) \end{pmatrix} \begin{pmatrix} y_1 \\ y_3 \\ \eta \end{pmatrix} = \tilde{A}(\mathrm{x}, \xi)\tilde{\mathrm{y}},$$

where

$$U_1 = \begin{pmatrix} x_1 + \alpha u_3 \\ x_2 + \alpha u_4 \end{pmatrix}, \quad U_2 = \begin{pmatrix} \beta u_3 \\ \beta u_4 \end{pmatrix}, \quad U_3 = \begin{pmatrix} \gamma u_3 \\ \gamma u_4 \end{pmatrix}, \quad U_4 = \begin{pmatrix} x_1 + \delta u_3 \\ x_2 + \delta u_4 \end{pmatrix},$$

$$A_1 = \begin{pmatrix} u_3 \\ u_4 \end{pmatrix}(a_1, a_2, \ldots, a_{s'}) \quad \text{and} \quad A_2 = \begin{pmatrix} u_3 \\ u_4 \end{pmatrix}(a_1', \ldots, a_{s'}').$$

Here s' is the number of ξ-indeterminants. The assumption that $L_1'(\mathrm{x}, \eta)$ depends on η_1 means that either $a_1 \neq 0$ or $a_1' \neq 0$. Assume $a_1 \neq 0$. The system $\mathscr{B}'$ satisfies $\bar{\mu}(\mathscr{B}') \leqslant \bar{\mu}(\mathscr{B}) - 2$.

We now define a system $\mathscr{B}''$, which is equivalent to $\mathscr{B}'$, by

$$\mathscr{B}'' = \begin{pmatrix} U_1 & U_2 & A_1 \\ U_3' & U_4' & A_2' \\ 0 & & A'(\xi) \end{pmatrix} \begin{pmatrix} y_1 \\ y_3 \\ \eta \end{pmatrix},$$

where

$$U_3' = U_3 - \frac{a_1'}{a_1} U_1 = \begin{pmatrix} \left(\gamma - \dfrac{\alpha a_1'}{a_1}\right) u_3 - \dfrac{a_1'}{a_1} x_1 \\ \left(\gamma - \dfrac{\alpha a_1'}{a_1}\right) u_4 - \dfrac{a_1'}{a_1} x_2 \end{pmatrix},$$

$$U_4' = U_4 - \frac{a_1'}{a_1} U_2 = \begin{pmatrix} x_1 + \left(\delta - \dfrac{a_1'}{a_1}\beta\right) u_3 \\ x_2 + \left(\delta - \dfrac{a_1'}{a_1}\beta\right) u_4 \end{pmatrix},$$

and

$$A'_2 = A_2 - \frac{a'_1}{a_1}A_1 = \begin{pmatrix} u_3 \\ u_4 \end{pmatrix}(a''_1, a''_2, \ldots, a''_{s'}).$$

By construction, $a''_1 = 0$.

We now claim that the four rows of the matrix

$$M = \begin{pmatrix} U_1 & U_2 & A_1 \\ U'_3 & U'_4 & A'_2 \end{pmatrix}$$

are G-linearly independent. Assume that for some $\mathbf{b}^T = (b_1, b_2, b_3, b_4)$ we have $\mathbf{b}^T M = 0$. Because the original matrix U was assumed to be definite, u_3 and u_4 are G-linearly independent. But the third column of M—the first column of $\begin{pmatrix} A_1 \\ A'_2 \end{pmatrix}$—is $(a_1u_3, a_1u_4, 0, 0)^T$, and therefore $b_1 = b_2 = 0$. So $\mathbf{b}^T M = 0$ implies $(b_3, b_4)U'_4 = 0$, which, by the definiteness of U, implies that $b_3 = b_4 = 0$.

Let us now substitute for the first four bilinear forms of $\mathscr{B}''$. The resulting system is

$$\mathscr{B}''' = \begin{pmatrix} V(\mathbf{x}, \boldsymbol{\xi}) & A'(\boldsymbol{\xi}) + N\begin{pmatrix} u_3 \\ u_4 \end{pmatrix} \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \\ \boldsymbol{\eta} \end{pmatrix},$$

where $V(\mathbf{x}, \boldsymbol{\xi})$ is $t' \times 2$ matrix whose entries are linear forms of $\mathbf{x}$ and $\boldsymbol{\xi}$ [here t' is the number of rows of $A'(\boldsymbol{\xi})$], and N is some $t' \times 2$ G-matrix. The system $\mathscr{B}'''$ satisfies $\bar{\mu}(\mathscr{B}''') \leqslant \bar{\mu}(\mathscr{B}'') - 4 = \bar{\mu}(\mathscr{B}') - 4 \leqslant \bar{\mu}(\mathscr{B}) - 6$.

Let $x_1 = L(\boldsymbol{\xi})$, $x_2 = L'(\boldsymbol{\xi})$ be the solution of $u_3 = u_4 = 0$. Our final modification is the system $\hat{\mathscr{B}}$, obtained from $\mathscr{B}'''$ by setting $x_1 = L(\boldsymbol{\xi})$, $x_2 = L'(\boldsymbol{\xi})$, $y_1 = y_3 = 0$. But now, $\bar{\mu}(A'(\boldsymbol{\xi})\boldsymbol{\eta}) = \bar{\mu}(\hat{\mathscr{B}}) \leqslant \bar{\mu}(\mathscr{B}''') \leqslant \bar{\mu}(\mathscr{B}) - 6$, which proves the lemma. ■

We now turn our attention to the case that U is not definite.

LEMMA 5.4. *Let $\mathscr{B}$ be the system*

$$\mathscr{B} = \begin{pmatrix} A(\mathbf{x}, \boldsymbol{\xi}) & 0 \\ \hat{A}(\mathbf{x}) & A'(\boldsymbol{\xi}) \end{pmatrix}\begin{pmatrix} \mathbf{y} \\ \boldsymbol{\eta} \end{pmatrix},$$

where $A(\mathbf{x}, \boldsymbol{\xi})$ *is a* $t \times s$ *matrix whose entries are linear forms in* $\mathbf{x}$ *and* $\boldsymbol{\xi}$, $\hat{A}(\mathbf{x})$ *is a* $t' \times s$ *matrix whose entries are linear forms in* $\mathbf{x}$, *and* $A'(\boldsymbol{\xi})$ *is a* $t' \times s'$ *matrix whose entries are linear forms in* $\boldsymbol{\xi}$. *If all the* s *columns of* $A(\mathbf{x}, \boldsymbol{\xi})$ *are G-linearly independent, then* $\bar{\mu}(\mathscr{B}) \geqslant s + \bar{\mu}(A'(\boldsymbol{\xi})\boldsymbol{\eta})$.

Proof. By assumption, $\mathscr{B}$ depends on $\{y_1, y_2, \ldots, y_s\}$. Substituting for $\{y_1, y_2, \ldots, y_s\}$, we obtain the system

$$\mathscr{B}' = \begin{pmatrix} A(\mathbf{x}, \boldsymbol{\xi})M \\ A'(\boldsymbol{\xi}) + \hat{A}(\mathbf{x})N \end{pmatrix}\boldsymbol{\eta},$$

where M, N are some $s \times s'$ G-matrices, and $\bar{\mu}(\mathscr{B}') \leqslant \bar{\mu}(\mathscr{B}) - s$.

Now, let $\mathscr{B}''$ be the system $\mathscr{B}'' = [A'(\boldsymbol{\xi}) + \hat{A}(\mathbf{x})N]\boldsymbol{\eta}$, then clearly $\bar{\mu}(\mathscr{B}'') \leqslant \bar{\mu}(\mathscr{B}')$. Finally, let $\mathscr{B}'''$ be the system obtained from $\mathscr{B}''$ by setting all the x_i's to be zero. We then obtain $\bar{\mu}(A'(\boldsymbol{\xi})\boldsymbol{\eta}) = \bar{\mu}(\mathscr{B}''') \leqslant \bar{\mu}(\mathscr{B}) - s$, which is the desired result. ∎

LEMMA 5.5. *Let* $\mathscr{B}$ *be the system*

$$\mathscr{B} = \begin{pmatrix} A(\mathbf{x}) \\ A'(\mathbf{x}; \boldsymbol{\xi}) \end{pmatrix}\mathbf{y},$$

where $A(\mathbf{x})$ *is a* $t \times s$ *matrix, and* $A'(\mathbf{x}; \boldsymbol{\xi})$ *is a* $t' \times s$ *matrix. If the* t *rows of* $A(\mathbf{x})$ *are G-linearly independent, then* $\bar{\mu}(\mathscr{B}) \geqslant \bar{\mu}(A'(0, \boldsymbol{\xi})y) + t$. *Here* $A'(0, \boldsymbol{\xi})$ *is obtained from* $A'(\mathbf{x}, \boldsymbol{\xi})$ *by setting all the* x_i*'s to be zero.*

Proof. The assumption that the t rows of $A(\mathbf{x})$ are G-linearly independent enables us to substitute for $A(\mathbf{x})\mathbf{y}$ in $\mathscr{B}$. This substitution yields a system $\mathscr{B}' = [A'(\mathbf{x}, \boldsymbol{\xi}) + MA(\mathbf{x})]\mathbf{y}$, for some $t' \times t$ G-matrix M. We also have $\bar{\mu}(\mathscr{B}') \leqslant \bar{\mu}(\mathscr{B}) - t$. Setting all the x_i's to be zero, we obtain $\bar{\mu}(A'(0, \boldsymbol{\xi})\mathbf{y}) \leqslant \bar{\mu}(\mathscr{B}') \leqslant \bar{\mu}(\mathscr{B}) - t$, which is what we had to prove. ∎

LEMMA 5.6. *Let*

$$U = \begin{pmatrix} x_1 & u_3(x_1, x_2; \boldsymbol{\xi}) \\ x_2 & u_4(x_1, x_2; \boldsymbol{\xi}) \end{pmatrix}$$

be a matrix which is not definite, and such that $u_3(x_1, x_2; \boldsymbol{\xi})$ *or* $u_4(x_1, x_2; \boldsymbol{\xi})$

depends on some ξ_i. *Let* $\mathscr{B}$ *be the system*

$$\mathscr{B} = \begin{pmatrix} U & 0 & 0 \\ 0 & U & 0 \\ 0 & 0 & A'(\xi) \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ \eta \end{pmatrix}.$$

Then $\bar{\mu}(\mathscr{B}) \geqslant \bar{\mu}(A'(\xi)) + 6$.

Proof. By assumption, there exist nonzero G-vectors $\mathbf{a} = (a_1, a_2)^T$ and $\mathbf{b} = (b_1, b_2)^T$ such that $0 = \mathbf{a}^T U \mathbf{b} = b_1(a_1 x_1 + a_2 x_2) + b_2(a_1 u_3 + a_2 u_4)$. Now, $b_2 \neq 0$, for otherwise $a_1 = a_2 = 0$, and so we may assume that $b_2 = 1$. With no loss of generality, we also assume that $a_1 \neq 0$, and in fact that $a_1 = 1$.

We now construct a new system $\mathscr{B}'$, which is equivalent to $\mathscr{B}$, by replacing U with

$$\begin{pmatrix} 1 & a_2 \\ 0 & 1 \end{pmatrix} U \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x_1 + a_2 x_2 & 0 \\ x_2 & b_1 x_2 + u_4 \end{pmatrix},$$

because by assumption $b_1(x_1 + a_2 x_2) + (u_3 + a_2 u_4) = 0$. This assumption also implies that u_4 depends on some ξ_i.

Therefore the system

$$\mathscr{B}'' = \begin{pmatrix} U' & 0 & 0 \\ 0 & U' & 0 \\ 0 & 0 & A'(\xi) \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ \eta \end{pmatrix}, \qquad \text{where} \quad U' = \begin{pmatrix} x_1 & 0 \\ x_2 & u_4' \end{pmatrix},$$

is equivalent to $\mathscr{B}$. Here $u_4' = u_4'(x_1, x_2; \xi)$ depends on some ξ_i.

We now apply lemma 5.5 to $\mathscr{B}''$, with $\{x_1\}$ playing the role of x, $\{x_2, \xi\}$ playing the role of ξ, and $\{y_1, y_2, y_3, y_4, \xi\}$ playing the role of y, and we obtain that

$$\mathscr{B}''' = \left(\begin{array}{cccc|c} x_2 & \hat{u}_4 & 0 & 0 & 0 \\ 0 & 0 & x_2 & \hat{u}_4 & \\ \hline \multicolumn{4}{c|}{0} & A'(\xi) \end{array}\right) \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ \eta \end{pmatrix}$$

satisfies $\bar{\mu}(\mathscr{B}''') \geqslant \bar{\mu}(\mathscr{B}) - 2$. Here $\hat{u}_4 = \hat{u}_4(x_2; \xi)$ is obtained from $u_4' = u_4'(x_1, x_2; \xi)$ by setting $x_1 = 0$.

We now apply Lemma 5.4 to $\mathscr{B}'''$, and we obtain $\bar{\mu}(A'(\xi)) \leqslant \bar{\mu}(\mathscr{B}''') - 4 \leqslant \bar{\mu}(\mathscr{B}) - 6$. This proves the lemma. ∎

Lemma 5.3 and Lemma 5.6 provide us with the results needed to prove the main theorem of this section.

THEOREM 5.1. *Let $A'(\xi)\eta$ be any system of bilinear forms. If $|G| \geqslant 3$, then $\langle 2,2,2\rangle$ and $A'(\xi)\eta$ satisfy the direct sum conjecture strongly.*

Proof. Let $\mathscr{A} = (m_1(x, \xi; y, \eta), \ldots, m_n(x, \xi; y, \eta))$ be a minimal algorithm for computing $\langle 2,2,2\rangle \oplus A'(\xi)\eta$. Clearly $n \leqslant \bar{\mu}(\langle 2,2,2\rangle) + \bar{\mu}(A'(\xi)\eta) = \bar{\mu}(A'(\xi)\eta) + 7$. We want to show that $\mathscr{A}$ is a direct sum algorithm, and therefore that equality holds.

Assume $\mathscr{A}$ is not a direct sum algorithm. By Lemma 2.2, $\mathscr{A}$ mixes x and ξ, so without loss of generality we assume that $L_1(x, \xi)$ depends on some x_i, say x_3, as well as on some ξ_i. We represent $\langle 2,2,2\rangle$ by

$$\begin{pmatrix} B_1 & B_3 \\ B_2 & B_4 \end{pmatrix} = \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix} \begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix}.$$

Here, as elsewhere in the paper, we assume that $m_i(x, \xi; y, \eta) = L_i(x, \xi)L_i'(y, \eta)$, $1 \leqslant i \leqslant n$.

Because $\mathscr{B} = \langle 2,2,2\rangle \oplus A'(\xi)\eta$ depends on $\{x_3, x_4\}$, we may assume that $L_1(x, \xi)$ and $L_2(x, \xi)$ depend on $\{x_3, x_4\}$. Let $\mathscr{B}'$ be the system obtained from $\mathscr{B} = \langle 2,2,2\rangle \oplus A'(\xi)\eta$ by substituting for $\{x_3, x_4\}$ in $L_1(x, \xi)$ and $L_2(x, \xi)$. The system $\mathscr{B}'$ is of the form

$$\mathscr{B}' = \begin{pmatrix} U & 0 & 0 \\ 0 & U & 0 \\ 0 & 0 & A'(\xi) \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ \eta \end{pmatrix}, \qquad \text{where} \quad U = \begin{pmatrix} x_1 & u_3(x_1, x_2; \xi) \\ x_2 & u_4(x_1, x_2; \xi) \end{pmatrix}.$$

The assumption that $L_1(x, \xi)$ depends on ξ_i implies that either $u_3(x_1, x_2; \xi)$ or $u_4(x_1, x_2; \xi)$ depends on ξ_i. The system $\mathscr{B}'$ satisfies $\bar{\mu}(\mathscr{B}') \leqslant \bar{\mu}(\mathscr{B}) - 2 = n - 1 \leqslant \bar{\mu}(A'(\xi)\eta) + 5$.

This last statement gives us a contradiction. If U is definite, it contradicts Lemma 5.3, and if U is not definite, it contradicts Lemma 5.6. Therefore $\mathscr{A}$ is a direct sum algorithm, which is what the theorem asserts. ∎

As was mentioned in Section III, the system $\mathscr{B}_Q$ of quaternion multiplication is equivalent to $\langle 2,2,2\rangle$ when G includes the field $\mathbb{Q}(i)$ of the rational numbers extended by $\sqrt{-1}$. So an immediate consequence of Theorem 5.1 is:

COROLLARY 5.1. *If $G \supseteq \mathbb{Q}(i)$ and $A'(\xi)\eta$ is a system of bilinear forms, then $\mathscr{B}_Q$ and $A'(\xi)\eta$ satisfy the direct sum conjecture strongly.*

Let H be a finite group. The system $\mathscr{B}_H = \{B_k | k \in H\}$ is defined by

$$\sum_{h \in H} b_k \cdot h = \Big(\sum_{h \in H} x_k \cdot h \Big) \Big(\sum_{h \in H} y_k \cdot h \Big).$$

Let $\{\rho_1, \rho_2, \ldots, \rho_r\}$ be the irreducible representations of H (over the field G), and let d_i be the dimension of ρ_i, $1 \leqslant i \leqslant r$. The system $\mathscr{B}_H$ is equivalent to $\oplus_{i=1}^{r} \langle d_i, d_i, d_i \rangle$, the r-fold direct sum of $d_i \times d_i$ "matrix multiplications." If all the d_i's are 1 or 2, then repeated use of Theorem 5.1 (for those d_i's which are 2) and Corollary 3.2 (for those d_i's which are 1) enables us to compute $\bar{\mu}(\mathscr{B}_H)$. For example:

COROLLARY 5.2 (Alder and Strassen). *Let D_m be the dihedral group of $2m$ elements, i.e. the group generated by a, b satisfying the relations $a^m = b^2 = 1$, $ba = a^{-1}b$. If G includes $\mathbb{Q}(w)$, where $w = e^{2\pi i/m}$, then*

$$\bar{\mu}(\mathscr{B}_{D_m}) = \begin{cases} 2 + \frac{7}{2}(m-1) & \text{if } m \text{ is odd}, \\ 4 + \frac{7}{2}(m-2) & \text{if } m \text{ is even}. \end{cases}$$

Proof. It is well known (see, for example, p. 339 of [10]) that, under the assumption on G, if m is odd D_m has 2 one dimensional representations and $(m-1)/2$ two dimensional representations, and if m is even D_m has 4 one dimensional representations and $(m-2)/2$ two dimensional representations. The lemma follows from Theorem 5.1 and Corollary 3.2. ∎

REMARK 5.1. This result has been recently obtained by A. Alder and V. Strassen using different techniques [8].

COROLLARY 5.3. *Let D_m and G be as in Lemma 5.2. For any $A'(\xi)\eta$, $\mathscr{B}_{D_m}$ and $A'(\xi)\eta$ satisfy the direct sum conjecture strongly.*

REFERENCES

1 V. Strassen, Vermeindung von Divisionen, *J. Reine Angew. Math.* 264:184–202 (1973).

2 C. M. Fiduccia and Y. Zalcstein, Algebras having linear multiplicative complexities, Rept. No. 46, Dept. of Computer Science, SUNY at Stony Brook, 1975; *J. Assoc. Comput. Mech.* 24:311–331 (1977).

3 J. Hopcroft and L. Kerr, On minimizing the number of multiplications necessary for matrix multiplication, *SIAM J. Appl. Math.* 20:30–36 (1971).

4 S. Winograd, Some bilinear forms whose multiplicative complexity depends on the field of constants, *Math. Systems Theory* 10:169–180 (1977).

5 L. Auslander, E. Feig, and S. Winograd, Direct sums of bilinear algorithms, *Linear Algebra Appl.*, to appear.

6 L. Auslander and S. Winograd, The multiplicative complexity of certain semilinear systems defined by polynomials, *Adv. in Appl. Math* 1:257–299 (1980).

7 E. Feig, Certain systems of bilinear forms whose minimal division-free algorithms are all quadratic, *Linear Algebra Appl., to appear.*

8 A. Alder and V. Strassen, On the algorithmic complexity of associative algebras, *Theoret. Comput. Sci.* 15:201–211 (1981).

9 S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965, p. 63.

10 C. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience, 1962.

11 H. F. de Groote and J. Heintz, Commutative algebras of minimal rank, *Linear Algebra Appl.*, to appear.

Received 31 May 1983; revised 22 November 1983